What is claimed is:

1. A secure adapter to transfer key code input from a keyboard to a computer system, characterized in a configuration to transfer input from the keyboard to the computer system after encryption if a secure mode setup command is received from the keyboard or the computer system, and to transfer the input from the keyboard to the computer system without encryption if a secure mode clearing command is received or under cleared secure mode.

2. A secure adapter according to Claim 1, further comprising:

a main processor to process the secure mode setup/clear command and to create a secrete key in setting secure mode;

an initial cipher to encrypt the secrete key transferred from the main processor with the secure key from the computer system and then to transfer the encrypted secrete key to the computer system; and

a stream cipher to encrypt the key code input information from the keyboard with the secrete key and then to transfer the encrypted information to the computer system.

3. A secure adapter according to Claim 1, further comprising:

a computer connection coupled to a keyboard port of the computer;

a keyboard connection coupled to a keyboard plug;

a transmit/receive control on the computer to control communication with the computer system;

a transmit/receive control on the keyboard to control communication with the

keyboard;

a main processor to create a secrete key, to perform secure mode setup/clearing according to the secure mode related commands, and to inter-transmit information of the computer system and the keyboard;

an initial cipher to encrypt the secrete key from the main processor with a secure key from the computer system and then to transmit the encrypted secrete key to the computer system, under secure mode; and

a stream cipher to encrypt the key code input information with the secrete key from the main processor and then to transmit the encrypted information to the computer system, under secure mode.

4. The secure adapter according to Claim 1, further comprising a built-in secure mode indication lamp which is ON under secure mode, OFF under cleared secure mode, and periodically blinks under disabled secure mode.

5. The secure adapter according to any one of Claims 1 through 4, further employing safe memory operation under the secure mode set by an application program executed in the computer system, said safe memory comprising:

a safe memory interface to transmit a password transmitted from the main processor, or the password and the data which requires security ("secure data"), to an encryption/key operation processor, and to transmit the data received from a decoder to the main processor;

an encryption/key operation processor to convert the password to the key ("the safe key"), and then, if the secure data is not received together with the password from the safe memory interface, to transmit the safe key to the decoder and to encrypt the

password with the safe key by encryption algorithm and calculate the integrity identification value of the encrypted password ("password integrity identification value") and then to transmit the password integrity identification value to a comparison/processor, and, if the secure data is received together with the password from the safe memory interface, to encrypt the secure data with the safe key and calculate the integrity identification value of the encrypted secure data ("encrypted data integrity identification value") and then to transmit the encrypted data integrity identification value together with the "encrypted data" to the comparison/processor;

a comparison/processor to transmit the stored data to the decoder if two integrity identification values are the same after comparing the "password integrity identification value" received from the encryption/key operation processor with the "password integrity identification value" stored in the data storage memory, to transmit password nonconformity to the computer and delete the temporally stored safe key on the decoder if the values are not the same, and to transmit the data to the data storage memory where "encrypted data" and "encrypted data integrity identification value" together with "password integrity identification value" are received from the encryption/key operation processor;

a data storage memory to store the encrypted data, the encrypted data integrity identification value and the password integrity identification value; and

a decoder to decode the encrypted data from the data storage memory with the safe key and then to transmit the decoded data to the safe memory interface,

wherein, where the said safe memory is employed, the main processor additionally has the function to transmit the password input request command to the computer system, and to transmit the password received from the keyboard to the safe memory, if the secure mode setup command received from the application program of

the computer system is for the safe memory.

6. The secure adapter as claimed in Claim 5, where the said integrity identification value is calculated using the CRC algorithm.

7. A computer secure system comprising the secure adapter, the keyboard and the computer system according to any one of Claims 1 through 6, where a separate secure key for entering secure mode setup/clearing command is incorporated in said keyboard and/or the secure mode setup/clearing command can be created by the combination of existing key codes, the computer system has the secure key creation function, the encryption/decoding function with the secrete key and the encryption/decoding function with the secure key, and the keyboard manager with application program interface is included.

8. A method to secure key code input information comprising the steps of:

transferring a secure key created in the keyboard manager of the computer system to the secure adapter in computer booting;

creating a new secrete key in the main processor when the secure mode setup command from the keyboard or the computer system is transferred to the main processor of the secure adapter, and then transferring the secrete key to the initial cipher and the stream cipher of the secure adapter;

encrypting the secrete key with the secure key in the initial cipher and then transferring the encrypted secrete key to the keyboard manager through the computer connection by the transmit/receive control on the computer;

under secure mode, main processor transferring the information to the stream

cipher if the key code input information of the keyboard is transferred to the main processor through the transmit/receive control on the keyboard, the stream cipher's encrypting the key code input information with the secrete key and transferring the encrypted information to the keyboard manager through computer connection by the transmit/receive control on the computer;

computer system decoding the encrypted information using the secrete key;

main processor transferring the secure mode clearing command to the stream cipher when the secure mode clearing command is transferred from the keyboard or the computer system to the main processor of the secure adapter; and

when secure mode is cleared, the stream cipher transferring the transferred key code input information to the keyboard manager through the computer connection by the transmit/receive control on the computer without encryption, if the key code input information of the keyboard is transferred to the stream cipher through the transmit/receive control on the keyboard after passing through the keyboard connection.

9. The method according to Claim 8, further characterized in that the decoding function using said secrete key is served by said keyboard manager of the computer system, or the operating system and/or application programs.

10. The method according to Claim 8, further characterized in that a protocol for acquiring decoded data exists between the keyboard manager and the application program, and between the keyboard manager and the application program.

11. The method according to Claim 8, further comprising the steps of:

main processor transferring the password from the transmit/receive control on

the keyboard and the secure data from the transmit/receive control on the computer to the safe memory after the main processor transfers the password input request command to the computer system, and safe memory encrypting and then storing the received data using the password, if secure mode setup is made by the command from the application program of the computer system and also for data storage requiring security; but

main processor transferring the password from the transmit/receive control on the keyboard to the safe memory after the main processor transfers the password input request command to the computer system, and safe memory decoding the encrypted data with the password and then transferring the decoded data to the main processor where the password is correct, but not decoding the encrypted data where not correct, if secure mode setup is made by the command from the application program of the computer system and also for acquisition of the secure data.